PROPEDÉUTICO DE MATEMÁTICAS

Generación 13

[2019]

Luis J. Dominguez Perez

GOBIERNO DE MÉXICO

Sesión 3

Contenido, sección 1

Grupos, anillos, polinomios, y campos finitos

Vectores

Matrices

Estructuras algebraicas

CIMAT

- Las estructuras algebraicas son el corazón de la mayoría de los criptosistemas y de los ataques criptoanalíticos.

- Sea G un conjunto de elementos, y $+, \times, \odot$ operadores binarios mapeando G a G, recordando las propiedades básicas discutidas en el inicio, tenemos que...

Objetos básicos

Los objetos matemáticos básicos son:

- Semigrupo: $\langle G, \odot \rangle$ es un semigrupo si G es cerrado y asociativo bajo $\odot$
- Monoide: $\langle G, \odot \rangle$ es un monoide si es un semigrupo, y existe un elemento identidad $e \in G$
- Grupo: $\langle G, \odot \rangle$ es un grupo si es un monoide, y existe un inverso para todo $a \in G$.
- Grupo abeliano: $\langle G, \odot \rangle$ es un grupo abeliano si es un grupo, y si $\odot$ es conmutativo
- Anillo: $\langle G, +, \times \rangle$ es un anillo si $\langle G, + \rangle$ es un grupo abeliano con identidad 0, $\langle G - \{0\}, \times \rangle$ es un monoide con identidad 1, y mantiene la propiedad distributiva bajo $+$
- Campo: $\langle G, +, \times \rangle$ es un campo si es un anillo, y $\langle G - \{0\}, \times \rangle$ es un grupo abeliano.

Ejemplos de estructuras algebraicas

CIMAT

Estructura	Monoide	Grupo	G. Abeliano	Anillo	A. Conmutativo	Campo
$\langle \mathbb{Q}^{n\times n}, \times \rangle$	✓	×	×	×	×	×
$\langle \mathbb{Q}^{n\times n}(inv), \times \rangle$	✓	✓	×	×	×	×
$\langle \mathbb{Z}, + \rangle$	✓	✓	✓	×	×	×
$\langle \mathbb{Q}^{n\times n}, +, \times \rangle$	–	–	–	✓	×	×
$\langle \mathbb{Z}/(15)\mathbb{Z}, +, \times \rangle$	–	–	–	✓	✓	×
$\langle \mathbb{Z}/(17)\mathbb{Z}, +, \times \rangle$	–	–	–	✓	✓	✓

- Las estructuras más utilizadas son los campos infinitos: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- En criptografía, las estructuras más utulizadas son las estructuras finitas, principalmente los grupos abelianos y los campos.

Observaciones sobre las estructuras

- En el caso de la criptografía, los campos utilizados son los *Campos Finitos* (también conocidos como *Campos de Galois*).
- Los campos finitos son los enteros módulo un primo p, o una potencia $q = p^m$, denotados como $\mathbb{F}_q$, o $\mathbb{Z}/q\,\mathbb{Z}$. Con $m \in \mathbb{Z}$, pudiendo ser un número compuesto.
- En el caso de ser una potencia prima, se les conoce como *extensión de campo*

observaciones

- Utilizar la q es una generalización para describir el campo finito. Algunos autores prefieres utilizar p, o la potencia explícita según les convenga.
- Un caso interesante es cuando el primo es 2, o 3. Adicionalmente, la potencia m compuesta por $2^i 3^j$, con $i, j \in \mathbb{Z}$, sin ser ambos cero, es popular.

- *Recientemente* se incluyen como estructuras algebraicas comunes a los grupos abelianos de puntos en curvas elípticas sobre un campo finito (o su extensión): $E(\mathbb{F}_p)$, $E_1(\mathbb{F}_{2^{1971}})$, $E'(\mathbb{F}_{p^d})$, ...

Ejercicio

- Defina campos finitos en Sage y verifique las propiedades algebraicas.

Subestructuras

Un subgrupo/campo es un subconjunto del conjunto original, el cual es cerrado bajo ciertas operaciones, y tiene las mismas propiedades que el original.

- Por ejemplo, $\mathbb{Z}/(15)\mathbb{Z}$ es un anillo, el subconjunto $\{0, 3, 6, 9, 12\}$ es cerrado, asociativo, y conmutativo bajo la adición, además, ya que tiene un elemento identidad, también es un subgrupo abeliano de $\mathbb{Z}/(15)\mathbb{Z}$ bajo la adición.

Orden

- Sea $\langle G, \odot \rangle$ un grupo con un elemento identidad e. El orden de G, escrito como $\text{ord}(G)$, u $|G|$ es el número de elementos en G. Si G es infinito, también lo es su orden.
- Otro tipo de orden existe para elementos en G. Si $a \in G$, entonces el orden de a es el entero positivo más chico $n > 0$, tal que:

$$\overbrace{a \odot a \odot \ldots \odot a}^{n \text{ times}} = 1$$

Si no existe n, entonces $\text{ord}(a) = \infty$.

Ejemplos

G	$\operatorname{ord}(G)$	a	$\operatorname{ord}(a)$
$\langle \mathbb{F}_{19}, \times \rangle$	18	7	3
$\langle \mathbb{F}_{19}, + \rangle$	19	7	19
$\langle \mathbb{F}_{17}, \times \rangle$	16	2	8
$\langle \{1, 3, 5, 9, 13\} \subset \mathbb{Z}/(14)\mathbb{Z}, \times \rangle$	6	11	3
$\langle \mathbb{Q}, \times \rangle$	∞	-1	2

Teorema

Si G es un grupo finito abeliano con elemento identidad 1, y $\beta \in G$, entonces:

$$\beta^{\text{ord}(G)} = 1$$

Sea $\text{ord}(G) = n$, $G = \{\alpha_i\}_{i=0}^{n-1}$, y $\beta G = \{\beta\alpha_i\}_{i=0}^{n-1}$. $\beta G = G$ dado que:

- G es cerrado, por lo que: $\beta G \subseteq G$
- $\beta - 1\alpha_i \in G$, por lo que $\beta\beta - 1\alpha_i = \alpha_i \in \beta G$, por lo que $G \subseteq \beta G$, y $G \subseteq \beta G$.

$$\prod_{i=0}^{n-1} \alpha_i = \prod_{i=0}^{n-1} \beta\alpha_i$$

$$\prod_{i=0}^{n-1} \alpha^{-1} \prod_{i=0}^{n-1} \alpha_i = \beta^n \prod_{i=0}^{n-1} \alpha - 1 \prod_{i=0}^{n-1} \alpha_i$$

$$1 = \beta^n$$

Por lo que $\beta^{\text{ord}(G)} = 1$.

Generadores

- Si el orden de un elemento equivale al orden del grupo, se dice que ese elemento es *primitivo*, o *generador*. Por ejemplo, $3 \in \mathbb{F}_7$:

i	1	2	3	4	5	6
3^i	3	2	6	4	5	1

  Los generadores solo existen en algunos anillos finitos: $\mathbb{F}_2$, $\mathbb{F}_p$, $\mathbb{F}_{p^n}$, o $\mathbb{F}_{2^n}$, $\mathbb{Z}/4\mathbb{Z}$, o $\mathbb{Z}/(2p)\mathbb{Z}$, donde p es un primo impar.

- Los grupo finitos que tienen generadores se llaman *grupos finitos cíclicos*, ya que forman un ciclo simple conteniento cada elemento.

Encontrando generadores

Cuando existen generadores, se pueden encontrar seleccionando $\alpha \in_R G$, y probando su orden.

- Sea $\alpha \in G$, $\text{ord}(G) = \prod_{i=0}^{n-1} p_i^{e_i}$, $0 < e_i$, y $\{p_i\}_{i=0}^{n-1}$ primos distintos.
- Dado que el orden de cualquier elemento en G divide $\text{ord}(G)$, podemos escribir: $\text{ord}(\alpha) = \prod_{i=0}^{n-1} p_i^{s_i}$ con $0 \leq s_i \leq e_i$.
- Elevando α a la $\frac{\text{ord}(G)}{p_i}$, tenemos que:

$$\alpha^{\frac{\text{ord}(G)}{p_i}} = \begin{cases} 1 & p^{e_i} \nmid \text{ord}(\alpha) \Rightarrow s_i < e_i \\ \text{de otro modo} & p^{e_i} \mid \text{ord}(\alpha) \Rightarrow s_i = e_i \end{cases}$$

Encontrando generadores

- Si $\alpha^{\frac{\mathrm{ord}(G)}{p_i}} = 1$, then $\mathrm{ord}(\alpha) | \frac{\mathrm{ord}(G)}{p_i}$, o:

$$\frac{p_i^{e_i} \prod_{j \neq i} p_j^{e_j}}{\prod_{j=0}^{n-1} p_j^{s_j}} = p_i^{e_i - s_i - 1} \prod_j^{e_j - s_j} \in \mathbb{Z}$$

por lo que $e_i - s_i - 1 \geq 0$, $s_i < e_i$, y $p^{e_i} \nmid \mathrm{ord}(\alpha)$. Si $\alpha^{\frac{\mathrm{ord}(G)}{p_i}} \neq 1$, then $\mathrm{ord}(\alpha) \nmid \frac{\mathrm{ord}(G)}{p_i}$, o:

$$p_i^{e_i - s_i - 1} \prod_{j \neq i} p_j^{e_j - s_j} \notin \mathbb{Z}$$

Encontrando generadores

- así que $e_i - s_i - 1 < 0$, $s_i = e_i$, y $p^{e_i} | \text{ord}(\alpha)$. Si $\alpha^{\frac{\text{ord}(G)}{p_i}} \neq 1$ para todo $p_i | \text{ord}(G)$, entonces el $\text{ord}(\alpha) = \text{ord}(G)$, ¡por lo que α es un generador!

Ejemplo

Ejemplo, encontrar un generador en $\mathbb{F}_{101}$.

- La factorización de $\phi(101) = 2^2 5^2$
- Verificar las dos exponenciaciones: α^{50}, y α^{20}. Si ninguna es 1, entonces α es un generador

α	α^{50}	α^{20}	¿generador?
2	100	95	✓
3	100	84	✓
77	1	36	×
69	100	1	×
17	1	1	×

Uso práctico

- El orden de un elemento facilita la suma y multiplicación en los exponentes.
  - Dado que $a^{\text{ord}(a)} = 1$: $a^{t+\text{ord}(a)} = a^t$
- Cálculo del inverso: $a^{-1} = a^{\text{ord}(a)-1}$
  - $3^{-1 \bmod 6} \equiv 3^5 \equiv 5 \bmod 7$
- Raíces: si el $\text{MCD}(\text{ord}(a), r) = 1$, entonces $\sqrt[r]{a} = a^{r^{-1} \bmod \text{ord}(a)}$
  - $\text{ord}(2) = 3 \in \mathbb{F}_7$, entonces $\sqrt{2} = 2^{2^{-1} \bmod 3} \equiv 4 \bmod 7$

- Calcular el orden de otro elemento: si $b = a^t$, y el $\text{MCD}(t, \text{ord}(a)) = g$, entonces el entero más pequeño n en $b^n = 1$ es:

$$n = \text{ord}(b) = \frac{\text{ord}(a)}{\text{MCD}(t, \text{ord}(a))}$$

  - $\text{ord}(3) = 6 \in \mathbb{F}_7$, por lo que $\text{ord}(2) = \text{ord}(3^2) = \frac{6}{\text{MCD}(6,2)} = 3$

Ejercicio

- Haga un programa para calcular el orden multiplicativo de todos los elementos en $\mathbb{F}_{101}$

Extensión de campos

- Las extensiones de campos, o de anillos polinomiales generales, se utilizan extensamente en la teoría de la información, además de en la criptografía. Se utilizan principalmente en los códigos de corrección de errores (para detectar bits erróneos en la transmisión de datos), en el procesamiento de señales y otras más.
- En el caso de la criptografía, se utilizan en los registros lineares de retroalimentación (que veremos más adelante), en los generadores de números aleatorios, cifrado AES, curvas elípticas, etc.

- Las extensiones comienzan sobre un *campo base*, como $\mathbb{F}_p$, y después la "extienden" al añadirle la raíz de un polinomio (solución a una ecuación irreducible en un campo dado).
  - Los números complejos son una extensión de campo sobre los números reales con la raíz $f(x) = x^2 + 1$ agregada: $i = \sqrt{-1}$ es una raíz de $f(x)$, y las potencias de i se reducen (simplifican) utilizando la relación $f(i) = 0$, o $i^2 = i$.
  - El conjunto de polinomios sobre un anillo R, $R[x] = \{\sum_{i=-1\infty}^{\infty} a_i x^i | a_i \in R\}$, utilizando operaciones normales de polinomios como suma y multiplicación, forman un anillo

CIMAT

Definición

Sea R un anillo, y $R[x]$ el anillo de polinomios con elementos $g(x), h(x) \in R[x]$. Se dice que $g(x)$ divide a $h(x)$, si existe un $k(x) \in R[x]$ tarl que $g(x)k(x) = h(x)$.

Ejemplos

Divisibilidad de polinomios:

- $(x-2)(x+2) = (x^2-4)$
  - (x^2-4) factoriza sobre $\mathbb{Z}$, y sobre cualquier anillo sobre los enteros

- $\left(x+(-1)^{\frac{1}{2}}\right)\left(x-(-1)^{\frac{1}{2}}\right) = (x^2+1)$
  - (x^2+1) no factoriza sobre los enteros, y sólo se factorizaría sobre anillos conteniendo un elemento de orden 4. Si R es un campo, note que la fórmula cuadrática genera las raíces, factorizando el polinomio cuadrático.

Ejemplos

- $(x+2)^2 \equiv x^2 + x + 1 \bmod 3$
- $(x+3)(x+5) \equiv x^2 + x + 1 \bmod 7$

- Para $x^2 + x + 1$, la fórmula cuadrática es:

$$x = 2^{-1}\left(-1 \pm (-3)^{\frac{1}{2}}\right)$$

  - Para el campo $\mathbb{F}_7$ la raíz cuadrada de (-3) es ± 2, en $\mathbb{F}_3$ es cero, por lo que $x^2 + x + 1$ es factorizable en los dos campos.
  - En el caso de $\mathbb{F}_2$, 2 no tiene raíz cuadrada.
  - En el caso de $\mathbb{F}_5$ $(-3 \equiv 2)$ no es residuo cuadrático, así que no existen racíces para $x^2 + x + 1$, por lo que no es factorizable.

Extensiones de campo sobre campos finitos

CIMAT

- En lugar de agregar i, agregamos raíces de polinomios sobre un campo. Por ejemplo, si $\mathbb{F}_2$ se exitende al añadir una raíz de $f(x) = x^+x + 1$, y llamamos esa raíz α, entonces $f(\alpha) = \alpha^3 + \alpha + 1 = 0$, y $\alpha^3 \equiv \alpha + 1$.
- Cabe destacar que las operaciones en $\mathbb{F}_2$ son peculiares: los valores negativos y los positivos son equivalentes, por lo que $\alpha^3 \equiv \alpha + 1$.

Ejemplo

Potencias de α, en donde α es una raíz de $f(x) = x^3 + x + 1$ sobre $\mathbb{F}_2$:

i	α	α^2	α^3	α^4	α^5	α^6	α^7
α^i	α	α^2	$\alpha + 1$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$	$\alpha^2 + 1$	1

Extensiones de campo sobre campos finitos

CIMAT

- Los campos con p^n elementos, como $\mathbb{F}_{2^3}$ se llaman *extensiones de campos*. El grado de la extensión de campos es el grado del polinomio cuya raíz se va a agregar.

- Hay muchas maneras de representar elementos en una extensión de campo de grado n. Además de agregar una raíz formal, se puede representar utilizando vectores de longitud n módulo $\mathbb{F}_p$, o polinomios con grado menor a n. Por ejemplo, $\alpha + 1$ se puede representar:
  - $[\ 0\ \ 0\ \ 0\ ]$
  - $(x+1)$

Suma

La suma es una simple adición vectorial directa, módulo p. Utilizando $\mathbb{F}_{2^3}$ como ejemplo, tenemos los 8 elementos del grupo:

$$\begin{bmatrix} 0 & 0 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 0 & 1 \end{bmatrix}$$
$$\begin{bmatrix} 0 & 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 & 1 \end{bmatrix}$$
$$\begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 1 \end{bmatrix}$$
$$\begin{bmatrix} 1 & 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$$

Así que la suma se hace así:

$$\begin{bmatrix} 0 & 1 & 0 \end{bmatrix} \oplus \begin{bmatrix} 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}$$

Multiplicación

- La multiplicación es máscomplicada. Si x se utiliza como una raíz de $f(x)$, los elementos módulo $f(x)$ se pueden interpretar como polinomios sobre $\mathbb{F}_p$.

- La multiplicación de elementos módulo $f(x)$ es una multiplicación polinomial simple, seguida de una reducción poinomial.

Ejemplo

- Sea el campo base $\mathbb{F}_5$, y $f(x) = x^4 + 4x^3 + 4$. Así que $x^4 \equiv x^3 + 1 \bmod f(x)$.
- Multiplicación de elementos en $\mathbb{F}_{5^4}$, $g(x) = x^3 + 2x + 3$, y $h(x) = 2x^2 + 4$.

En la primera fila se utiliza la notación polinomial estándar, mientras que en la segunda, se utilizan polinomios.

$g(x)$	$h(x)$	$g(x)h(x) \bmod f(x)$
$x^3 + 2x + 3$ $[\ 1\ \ 0\ \ 2\ \ 3\ ]$	$2x^2 + 4$ $[\ 0\ \ 2\ \ 0\ \ 4\ ]$	$(2x^5 + 4x^3 + x^2) + (4x^3 + 3x + 2)$ $[\ 0\ \ 0\ \ 2\ \ 0\ ] \cdot [\ 1\ \ 0\ \ 0\ \ 1\ ]$ $+[\ 3\ \ 1\ \ 3\ \ 2\ ] \cdot 2[\ 1\ \ 0\ \ 0\ \ 1\ ]$ $+[\ 3\ \ 1\ \ 0\ \ 2\ ] \cdot [\ 0\ \ 1\ \ 0\ \ 4\ ]$

Anillos y campos

Estas estructuras polinomiales forman anillos y campos dependiendo de la *irreducibilidad* del módulo.

- La estructura $\mathbb{Z}/(n)\mathbb{Z}$ es un anillo el entero compuesto n, y para el primo n; la misma estructura se mantiene para $\mathbb{Z}[x]/f(x)$.
- Si $f(x)$ es irreducible -divisible por los elementos del campo base y $f(x)$- entonces la estructura forma un campo.

Ejemplos

Campo base	$f(x)$	Irreducible	Factores
$\mathbb{F}_2$	x^2+x+1	✓	$\times$
$\mathbb{F}_3$	x^2+x+1	$\times$	$(x+2)^2$
$\mathbb{F}_5$	x^2+x+1	✓	$\times$
$\mathbb{F}_7$	x^2+x+1	$\times$	$(x+3)(x+5)$

Los polinomios *unitarios* (monic) tienen su coeficiente de mayor order igual a uno. Si el polnomio no es unitario, entonces se puede convertir al multiplicarlo por el inverso del término de mayor orden.

CIMAT

Observación

Cuando se utilizan polinomios como módulo o cuando se discute irreducibilidad, se asume que se está hablando de polinomios unitarios.

- Factorizar y verificar la irreducibilidad de los polinomios es trivial para grado $n \leq 3$. En estos casos, los polinomios deben de tener una raíz en el campo base, sino, son irreducibles.
- El polinomio $f(x)$ sobre $\mathbb{F}_p$ tiene una raíz r en el campo base: $f(r) \equiv 0 \bmod p$, sí y solo si $(x - r)$ divide a $f(x)$.
- Los polinomios de grado menor o igual a 3 tienen al menos un factor de grado 1, sino, son irreducibles.

Ejemplo

- $f(x) = x^2 + x + 1$ sobre $\mathbb{F}_7$ tiene una raíz en 4:
  $f(4) \equiv 0 \bmod 7$, y $(x - 4) \equiv (x + 3) \bmod 7$ divide a $f(x)$.
  - $(x + 3)x = x^2 + 3x$: $(x^2 + x + 1) - (x^2 + 3x) = -2x + 1$
  - $-2x + 1 \equiv 5x + 1 \bmod 7$
  - $(x + 3)5 = 5x + 15 \equiv 5x + 1$
- $(x + 3)(x + 5) | x^2 + x + 1$ en $\mathbb{F}_7$.

Polinomios primitivos y orden

- La reducción módulo un polinomio irreducible sobre un campo finito genera la extensión de campo de grado n, en donde n es el grado de dicho polinomio: $\mathbb{F}_{p^n}$

- Al igual que en el caso de los campos primos, las extensiones de campo tienen el concepto de orden, tanto para el grupo multiplicativo, como para los elementos individuales.

Contenido, sección 2

- Sea K un campo. Un **vector espacio** V sobre el campo K es un grupo aditivo (abeliano), junto con la multiplicación de elementos de V por elementos de K; i.e. una asociación

$$(x, \nu) \mapsto x\nu$$

de $K \times V$ hacia V, satisfaciendo las siguientes condiciones:

  - Si 1 es el elemento unidad e K, entonces $1\nu = \nu$ para todo $\nu \in V$
  - Si $c \in K$ y $\nu, w \in V$, entonces $c(\nu + w) = c\nu + cw$
  - Si $x, y \in K$ y $\nu \in V$, entonces $(x + y)\nu = x\nu + y\nu$
  - Si $x, y \in K$ y $\nu \in V$, entonces $(xy)\nu = x(y\nu)$

Subespacio

- Sea V un vector espacio y W un subconjunto de V. Decimos que W es un **subespacio** si W es un subgrupo (del grupo aditivo de V), y si dado $c \in K$ y $\nu \in W$ entonces $c\nu$ es también un elemento de W. En otras palabras, el subespacio W de V es un subconjunto que satisface las siguientes condiciones:
  - Si ν, w son elementos de W, su suma $\nu + w$ es también un elemento de W.
  - El elemento 0 de V es también un elemento de W
  - Si $\nu \in W$) y $c \in K$ entonces $cv \in W$

Entonces W es un vector espacio por sí mismo

Linealidad de elementos

- Sea V un vector espacio sobre un campo K, y sea $\nu_1, \ldots, \nu_n$ elementos de V. Debemos decir que $\nu_1, \ldots, \nu_n$ son **linealmente independientes sobre** K si existen elementos $a_1, \ldots, a_n$ en K no iguales a 0 tal que:

$$a_1\nu_1 + \cdots + a_n\nu_n = 0$$

Si no existen tales elementos, entonces decimos que $\nu_1, \ldots, \nu_n$ son **linealmente independientes sobre** K (o simplemente linealmente independiente).

Ejemplo

- Sea $V = K^n$ y considere los siguientes vectores:

$$\nu_1 = (1, 0, \ldots, 0)$$
$$\nu_2 = (0, 1, \ldots, 0)$$
$$\vdots$$
$$\nu_n = (0, 0, \ldots, 1)$$

Entonces $\nu_1, \ldots, \nu_n$ son linealmente independientes. De hecho, sean $a_1, \ldots, a_n$ elementos de K tal que $a_1\nu_1 + \cdots + a_n\nu_n = 0$, dado que

$$a_1\nu_1 + \cdots + a_n\nu_n = (a_1, \ldots, a_n)$$

entonces todo $a_i = 0$.

Base

- Definimos una **base** de V sobre K como una secuencia de elementos $\{\nu_1, \cdots, \nu_n\}$ de V, que generan a V y que son linealmente independientes.
- Sea V un vector espacio, y sea $\{\nu_1, \cdots, \nu_n\}$ una base de V. Los elementos de V se pueden representar xon n-tuplas relativas a esta base, como sigue. Si un elemento ν de V se escribe como una combinación lineal

$$\nu = x_1\nu_1 + \ldots + x_n\nu_n$$

de los elementos de la base, entonces llamamos $(x_1, \ldots, x_n)$ las **coordenadas** de ν respecto a su base, llamamos a x_i la i-ésima coordenada.

- Finalmente, decimos que la n-tupla $X = (x_1, \ldots, x_n)$ es el **vector coordenada** de ν con respecto a la base $\{\nu_1, \cdots, \nu_n\}$.

Maximal

- Sea $\{\nu_1, \cdots, \nu_n\}$ el conjunto de elementos de un vector espacio V sobre un campo K. Sea r un entero positivo $\leq n$. Debeos decir que $\{\nu_1, \cdots, \nu_n\}$ es un subconjunto **maximal** de elementos linealmente independientes si $\nu_1, \cdots, \nu_n$ son linealmente independientes y si, adicionalmente, dado cualquier ν_i on $i > r$, los elementos $\nu_1, \cdots, \nu_r, \nu_i$ son linealmente dependientes.

Esto es, que es el número máximo de elementos que hacen el subconjunto linealmente independiente, agregar otro provoca que haya dependencia lineal entre algunos de ellos.

- Sean V, W vectores espacio sobre K. Un mapa

$$f : V \to W$$

se le llama un **mapa K-lineal** o un **homomorfismo de vectores espacio** si f satisface la siguiente condición: Para todo $x \in K$ y $\nu, \nu' \in V$ tenemos

$$f(\nu + \nu') = f(\nu) + f(\nu'), \quad f(x\nu) = xf(\nu).$$

Kernel

- El **kernel** de un mapa linear es definido como el kernel del mapa, visto como un homomorfismo aditivo de grupos. Entonces, el *Kerf* es el conjunto de $\nu \in V$ tal que $f(\nu) = 0$

Esto es, que el resultado de la función f, con el vector ν de parámetro da 0.

- Sea $f : V \to W$ un mapa lineal. Si f es biyectivo, esto es, inyectivo y suryectivo, entonces f tiene un mapeo inverso:

$$g : W \to V$$

y si este es lineal y biyectivo, entonces también es un mapa lineal.

Isomorfismo

- Así como en grupos, decimos que si un mapa lineal $f : V \to W$ es un **isomorfismo** (isomorfismo de vectores espacio) si tiene un inverso lineal; i.e., existe un mapa lineal $g : W \to V$ tal que $g \circ f$ es la identidad de V y $f \circ g$ es la identidad de W.

Dimensión

- Si un vector tiene una base, entonces cualquier otra base tiene el mismo número de elementos. Este número se le conoce como la **dimensión** de V (sobre K). Si V es el vector 0, definimos a V con dimensión 0.

Contenido, sección 3

Definición

- Para enteros positivos m y n, una **matriz** A de $m \times n$ sobre un anillo R es un arreglo rectangular:

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix}$$

En donde cada entrada $a_{i,j}$ en el arreglo es un elemento de R; el elemento $a_{i,j}$ se llama **entrada** (i, j) de A, denotada como $A_{i,j}$.

- Nótese que en matemáticas primero van los renglones y después las columnas, lo opuesto que en las ciencias computacionales!

Renglón y Columna

- Para $i = 1, \ldots, m$, el i-**ésimo renglón** de A es:

$$(a_{i,1}, \ldots, a_{i,n}),$$

  denotado como $\textbf{Renglón}_i(A)$

- Para $j = 1, \ldots, n$, la j-**ésima columna** de A es:

$$\begin{pmatrix} a_{1,j} \\ \vdots \\ a_{m,j} \end{pmatrix}$$

  denotado como $\textbf{Columna}_j(A)$

Se dice que un renglón de A es una matriz de $1 \times n$, y una columna de A es una matriz de $m \times 1$.

Tamaños

- El conjunto de todas las matrices $m \times n$ sobre R se denota como $R^{m \times n}$.
- Los elementos de $R^{1 \times n}$ se llaman **vector renglón** (**de dimensión** n)
- Los elementos de $R^{m \times 1}$ se llaman **vector columna** (**de dimensión** m)
- Los elementos de $R^{n \times n}$ se llaman **matrices cuadradas** (**de dimensión** n)

Suma y multiplicación escalar

Definimos las operaciones de **adición de matrices** y **multiplicación escalar de matrices**

- Si $A, B \in R^{m \times n}$, entonces $A + B$ es la matriz $m \times n$ cuya entrada (i, j) es $A(i, j) + B(i, j)$
- Si $c \in R$ y $A \in R^{m \times n}$, entonces A es la matriz $m \times n$ cuya entrada (i, j) es $cA(i, j)$

Adicionalmente, definimos la **matrix cero** $m \times n$ a la matriz $m \times n$ cuyas entradas son todas 0_R, y se denota como $0_R^{m \times n}$

Identidades

- La matriz $0_R^{m\times n}$ es la identidad aditiva
- El inverso aditivo es la matriz $R^{m\times n}$ cuyas entradas (i,j) son $-A(i,j)$

Multiplicación de matrices

- Si $A \in R^{m \times n}$ y $B \in R^{n \times p}$, entonces AB es la matriz $m \times p$ cuya entrada (i, k) es:

$$\sum_{j=1}^{n} A(i,j)B(j,k)$$

Adicionalmente, definimos como la **matriz identidad** de $n \times n$ como la matriz $I \in R^{n \times n}$, en donde $I(i,i) = 1_R$ y $I(i,j) = 0_R$ para $i \neq j$.

Propiedades

- La multiplicación de matrices es asociativa: $A(BC) = (AB)C$ para toda $A \in R^{m\times n}$, $B \in R^{n\times p}$ y $C \in R^{p\times q}$
- La multiplicación de matrices es distributiva: $A(C + D) = AC + AD$ y $(A + B)C = AC + BC$ para toda $A, B \in R^{m\times n}$ y $C, D \in R^{n\times p}$
- La matriz identidad de $n \times n$ $I \in R^{n\times n}$ actúa como identidad de multiplicación: $AI = A$ e $IB = B$ para toda $A \in R^{m\times n}$ y $B \in R^{n\times m}$, en particular $CI = C = IC$ para toda $C \in R^{n\times n}$
- La multiplicación de matrices y la multiplicación escalar de matrices son asociativas: $c(AB) = (cA)B = A(cB)$ para toda $c \in R$, $A \in R^{m\times n}$ y $B \in R^{n\times p}$

Transpuesta

- Si $A \in R^{m \times n}$, entonces la **transpuesta** de A, denotada como A^T, se define como la matriz $n \times m$ cuya entrada $(j, i) = A(i, j)$.

Dados $A, B \in R^{m \times n}$, $C \in R^{n \times p}$ y $c \in R$, entonces

- $(A + B)^T = A^T + B^T$
- $(cA)^T = cA^T$
- $(A^T)^T = A$
- $(AC)^T = C^T A^T$